CUI / CDI
NIST SP 800-171
Onboarding

Initial information for Principal Investigators working with data requiring NIST SP 800-171 controls

Updated: July 02, 2018

Questions can be submitted to:
cui-support@list.arizona.edu
Outline

1. What is CUI / CDI / NIST SP 800-171?
2. AWS GovCloud Environment Overview
3. GovCloud S3 Bucket Application
4. Continuous Monitoring Overview
5. “Green” versus “Red” machines
6. CUI “Green” Laptop
7. System Hierarchy
What is CUI / CDI / NIST 800-171?

**Controlled Unclassified Information (CUI)**
Is federal non-classified data that federal agencies create or possess, or that a non-federal entity (e.g., UA) receives, possesses, or creates for, or on behalf of the federal government, which requires certain data security controls to safeguard or disseminate.

**Covered Defense Information (CDI)**
Data that is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of a DoD contract. DFARS 252.204-7012 promulgates CDI as CUI.

**NIST SP 800-171**
Defines 110 information security controls for protecting the confidentiality of CUI. These controls are mapped to the medium set of NIST 800-53 confidentiality controls.
Amazon Web Services GovCloud

- Amazon Web Services (AWS) offers reliable and scalable cloud RAM/CPU services
- The GovCloud region of AWS offers NIST SP 800-171 compliant security of the cloud
  - UA is still responsible for NIST SP 800-171 compliance in the cloud

AWS GovCloud Compute Environment

- Linux or Windows
- Custom storage / RAM / CPU / application installations
- Can be turned off when not being used (to save RAM / CPU costs)
Amazon Simple Storage Service (S3)
• Amazon S3 stores data as objects within resources called “buckets”
• We have configured our S3 buckets to encrypt data at rest according to FIPS 140-2, Level 2, requirements

S3 Bucket “Drop Box” Application
• UA developed application that sits on top of S3 bucket that allows a project sponsor to connect and retrieve data via two-factor authentication
  • Sponsor is required to have a Net ID, which is created as part of a Designated Campus Colleague (DCC) request using the specialized “Sponsored Research Authentication” (SRA) subtype
  • SRA DCC accounts can be requested by departments after following all applicable Export Control processes
Continuous Monitoring

Requirements

• All assets that store, process, or transmit CUI data, or provide security for such components are required to be continuously monitored for security incidents
  • There is a required 72 hour reporting window for reporting cyber incidents

Current Configuration

• All assets have Splunk agents send logs to a central aggregator in the AWS GovCloud environment
• Logs are continuously monitored by an external Security Operations Center (SOC)
  • Alerts are escalated to the UA Operations team
“Green” versus “Red” machines

**Green Machines**

- A UA-owned laptop that can **locally** store, process, or transmit CUI, or provide security protection for such components
- Green machines are IT/UITS managed assets that are in-scope for all 110 controls in the NIST SP 800-171.

**Red Machines**

- A laptop/desktop that **does not** locally store, process, or transmit CUI, or provide security protection for such components
- Red machines are unmanaged assets that may access the GovCloud environment by going through a terminal host.
**CUI “Green” Laptop**

- Capable of locally storing, processing, and transmitting CUI data
- In-scope for all 110 controls of the NIST SP 800-171
- To be used for CUI work only
- USB ports should not be utilized unless the device is specifically authorized by the project Technology Control Plan (TCP)
- Runs Windows 10 with NIST SP 800-171 required security hardening
- Requested through departmental IT Staff